PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-162859
(43)Date of publication of application : 20.06.1997

(51)Int.Cl. H04L 9/20
H04L 9/16
H04N 7/24
H04N 7/167

(21)Application number : 07-319421
(22)Date of filing : 07.12.1995

(71)Applicant : FUJITSU LTD
(72)Inventor : OGAWA KIYOTAKA
KOBIYAMA KIYOYUKI
AKIYAMA RYOTA
IIJIMA KIYOKATSU

(54) SCRAMBLING METHOD AND DEVICEDESCRAMBLING METHOD AND DEVICE AND DATA TRANSMISSION METHOD AND SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To realize data transmission with high security with respect to a data transmission system suitable for a transfer system of the MPEG standard stream.
SOLUTION: A PTS (time management information of a reproduction output) whose value is not definite is fed by each stream of packet data part being an object of scramble to a random number generator 24 of a scramble circuit 23 as an initial value and the PTS is fed to a random number generator 32 of a descramble circuit 31 as an initial value by each stream of packet data part to be scrambled.

CLAIMS

[Claim(s)]
[Claim 1]Inside of a stream which puts in a row a stream which arranged the 2nd stream part behind the 1st stream part as a unit streamIt is a scrambling method which carries out the scramble of the 2nd stream part made into an object of scramble using a random number generatorWhen said 1st data value of stream circles supplies said random number generator every 2nd stream part made into an object of said scramble by making into an initial value a data value of

predetermined data which is not constantA scrambling method carrying out the scramble of the 2nd stream part made into an object of said scramble.
[Claim 2]When said predetermined data does not exist in the 1st stream circles of the same unit stream as the 2nd stream part made into an object of said scrambleBy supplying said random number generator by making into an initial value a data value of said 1st predetermined data of stream circles in front of the 1st stream part in which said predetermined data does not exist among the 1st stream part in which said predetermined data existsThe scrambling method according to claim 1 carrying out the scramble of the 2nd stream part made into an object of said scramble.
[Claim 3]A stream which puts in a row a stream which arranged the 2nd stream part behind said 1st stream part as a unit stream is a standard stream for MPEG. Said 1st stream part a stream of a packet header unit and said 2nd stream partA stream of a packet data division or a payload partand said predetermined dataThe scrambling method according to claim 1 or 2 being combination or the calculated data about a presentation time stampa decoding time stampa round counteror a decoding time stamp and a round counter.

[Claim 4]The scrambling method according to claim 12or 3 carrying out parallel conversion of all or a part of streams which puts in a row a stream which arranged the 2nd stream part behind said 1st stream part as a unit stream to a stream of plural linesand carrying out scramble.
[Claim 5]Inside of a stream which puts in a row a stream which arranged the 2nd stream part behind the 1st stream part as a unit streamA random number generator which is a scramble device which carries out the scramble of the 2nd stream part made into an object of scrambleand generates a random numberAn initial value supply circuit supplied to said random number generator every 2nd stream part made into an object of said scramble by making into an initial value a data value of predetermined data said 1st data value of stream circles is not constantA scramble device provided with a logic operation circuit which carries out the scramble of the 2nd stream part that carries out the logical operation of the 2nd stream part made into an object of said scrambleand the random number outputted from said random number generatorand is made into an object of said scramble.
[Claim 6]When said predetermined data does not exist in the 1st stream circles of the same unit stream as the 2nd stream part made into an object of said scramblesaid initial value supply circuitThe scramble device according to claim 5 supplying said random number generator by making into an initial value a data value of said 1st predetermined data of stream circles in front of the 1st stream part in which said predetermined data does not exist among the 1st stream part in which said predetermined data exists.
[Claim 7]A stream which puts in a row a stream which arranged the 2nd stream part behind said 1st stream part as a unit streamAre a standard stream for MPEG and said 1st stream partA stream of a packet header unit and said 2nd streamA

stream of a packet data division or a payload partand said predetermined dataThe scramble device according to claim 5 or 6 being combination or the calculated data about a presentation time stampa decoding time stampa round counteror a decoding time stamp and a round counter.
[Claim 8]The scramble device comprising according to claim 56or 7:
A position detecting circuit where said initial value supply circuit detects a position of said predetermined dataand a starting position of said 2nd stream part.
A data holding circuit which holds a data value of said predetermined data when this position detecting circuit detects a position of said predetermined data.

[Claim 9]It has a serial/parallel-conversion circuit which carries out parallel conversion of the stream which puts in a row a stream which arranged the 2nd stream part behind said 1st stream part as a unit stream to a stream of plural linesSaid data holding circuit and said logic operation circuitThe scramble device according to claim 567or 8 being constituted so that it can respond to a stream of plural linesand having a parallel/serial-conversion circuit which carries out serial conversion of the stream of plural lines outputted from said logic operation circuit.
[Claim 10]The scramble device according to claim 8 or 9 constituting so that it can respond to several streams which perform processing by said position detecting circuit by software processing by CPUand from which a standard differs.
[Claim 11]Inside of a stream which puts in a row a stream which arranged the 2nd stream part behind the 1st stream part as a unit streamIt is the descrambling method which descrambles the 2nd stream part made into an object of descrambling using a random number generatorWhen said 1st data value of stream circles supplies said random number generator every 2nd stream part made into an object of said descrambling by making into an initial value a data value of predetermined data which is not constantA descrambling method descrambling the 2nd stream part made into an object of said descrambling.
[Claim 12]When said predetermined data does not exist in the 1st stream circles of the same unit stream as the 2nd stream part made into an object of said descramblingBy supplying said random number generator by making into an initial value a data value of said 1st predetermined data of stream circles in front of the 1st stream part in which said predetermined data does not exist among the 1st stream part in which said predetermined data existsA descrambling method according to claim 11 descrambling the 2nd stream part made into an object of said descrambling.
[Claim 13]A stream which puts in a row a stream which arranged the 2nd stream part behind said 1st stream part as a unit streamAre a standard stream for MPEG and said 1st stream partA stream of a packet header unit and said 2nd streamA stream of a packet data division or a payload partand said predetermined dataA descrambling method according to claim 11 or 12 being combination or the calculated data about a presentation time stampa decoding time stampa round counteror a decoding time stamp and a round counter.
[Claim 14]A descrambling method according to claim 1112or 13 carrying out

parallel conversion of all or a part of streams which puts in a row a stream which arranged the 2nd stream part behind said 1st stream part as a unit stream to two or more streamsand descrambling it.
[Claim 15]Inside of a stream which puts in a row a stream which arranged the 2nd stream part behind the 1st stream part as a unit streamA random number generator which is a descrambling device which descrambles the 2nd stream part made into an object of descramblingand generates a random numberAn initial value supply circuit supplied to said random number generator every 2nd stream part made into an object of said descrambling by making into an initial value a data value of predetermined data said 1st data value of stream circles is not constantA descrambling device provided with a logic operation circuit which descrambles the 2nd stream part that carries out the logical operation of the 2nd stream part made into an object of said descramblingand the random number outputted from said random number generatorand is made into an object of said descrambling.
[Claim 16]When said predetermined data does not exist in the 1st stream circles of the same unit stream as the 2nd stream part made into an object of said descramblingsaid initial value supply circuitThe descrambling device according to claim 15 supplying said random number generator by making into an initial value a data value of said 1st predetermined data of stream circles in front of the 1st stream part in which said predetermined data does not exist among the 1st stream part in which said predetermined data exists.
[Claim 17]A stream which puts in a row a stream which arranged the 2nd stream part behind said 1st stream part as a unit streamAre a standard stream for MPEG and said 1st stream partA stream of a packet header unit and said 2nd streamA stream of a packet data division or a payload partand said predetermined dataThe descrambling device according to claim 15 or 16 being combination or the calculated data about a presentation time stampa decoding time stampa round counteror a decoding time stamp and a round counter.
[Claim 18]The descrambling device comprising according to claim 1516or 17:
A position detecting circuit where said initial value supply circuit detects a position of said predetermined dataand a starting position of said 2nd stream part.
A data holding circuit which holds a data value of said predetermined data when this position detecting circuit detects a position of said predetermined data.

[Claim 19]It has a serial/parallel-conversion circuit which carries out parallel conversion of the stream which puts in a row a stream which arranged the 2nd stream part behind said 1st stream part as a unit stream to a stream of plural linesSaid data holding circuit and said logic operation circuitClaim 15 being constituted so that it can respond to a stream of plural linesand having a parallel/serial-conversion circuit which carries out serial conversion of the stream of plural lines outputted from said logic operation circuit16 and 17or a descrambling device given in 18.
[Claim 20]The descrambling device according to claim 18 or 19 constituting so that it can respond to several streams which perform processing by said position

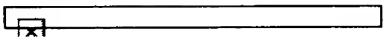
detecting circuit by software processing by CPUand from which a standard differs.
[Claim 21]The descrambling device according to claim 1516or 17 constituting so that said random number generator can be accessed from said external device only when it is card-izedand it has a store circuit which memorizes identification data and said identification data is attested from an external device.
[Claim 22]About a stream which puts in a row a stream which arranged the 2nd stream part behind the 1st stream part to a transmitting agency as a unit stream. Perform the scrambling method according to claim 123or 4and a stream obtained by this is transmitted to a transfer place via transfer mediaIn said transfer placea descrambling method according to claim 111213or 14 is performedA data transmission method including a process of restoring a stream which puts in a row a stream which arranged the 2nd stream part as a unit stream behind said 1st stream part.
[Claim 23]A data transmitting system comprising:
It has the scramble device according to claim 56789or 10Transfer origin which is changed into a stream which carries out the scramble of the 2nd stream part for which a stream which puts in a row a stream which arranged the 2nd stream part behind the 1st stream part as a unit stream is set as the object of scrambleand is transmitted to transfer media.
A transfer place which restores a stream which arranged the 2nd stream part for a stream which has the descrambling device according to claim 151617181920or 21and is supplied from said transfer media behind said 1st stream part to a stream put in a row as a unit stream.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention Digital video coding (compression)Apply to the transmission system etc. of the standard stream (bit string) for MPEG (Moving Picture Experts Group) which is the international standards about sound codingand multiplex and the separation method for the sameand in a suitable scrambling method and devicethe descrambling method and a deviceand a row. It is related with the data transmission method and a system.
[0002]
[Description of the Prior Art]Conventionallythe thing as shows drawing 12 the important section is known as a data transmitting systemfor example.
[0003]A microphone for a camera for one to obtain picture image data among drawing 12 and 2 to obtain voice dataThe packet header unit which 3 coded and carried out Time Division Multiplexing of the picture image data obtained with the camera 1and the voice data obtained with the microphone 2and arranged attached dataIt is an MPEG encoder encoded to the standard stream for MPEG which

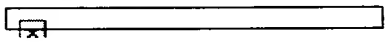
consists of a packet data division which arranged picture image data and voice data.
[0004]4 is a scramble circuit where the stream of a packet data division changes the stream outputted from MPEG encoder 3 into the stream which comes to carry out scramble.
[0005]The random number generator which generates the random number of the series as which 5 is specified by a key signal in this scramble circuit 46 is an EOR circuit which carries out exclusive OR (henceforth EOR) processing of the stream of the packet data division of the streams outputted from MPEG encoder 3and the random number outputted from the random number generator 5.
[0006]7 is a selection circuitry which chooses and outputs the stream of the packet header unit of the streams outputted from MPEG encoder 3and the stream outputted from EOR circuit 6.
[0007]8 is transfer media which are the transmission media of the stream outputted from the scramble circuit 4such as broadcasting mediasuch as storage mediasuch as a disk and a tapesatellite broadcastingCATV.
[0008]9 is a descramble circuit where the stream of a packet data division changes the stream outputted from the scramble circuit 4 transmitted via the transfer media 8 into the stream which it comes to descramble.
[0009]In this descramble circuit 910 is a random number generator of the same circuitry as the random number generator 5and the key signal and the key signal of an identical content which were used for the random number generator 5 are supplied to this random number generator 10.
[0010]11 is an EOR circuit which carries out EOR processing of the stream of the packet data division of the streams outputted from the scramble circuit 4 transmitted via the transfer media 8and the random number outputted from the random number generator 10.
[0011]12 is a selection circuitry which chooses and outputs the stream of the packet header unit of the streams outputted from the scramble circuit 4 transmitted via the transfer media 8and the stream outputted from EOR circuit 11.
[0012]13 separates picture image data and voice data from the stream outputted from the descramble circuit 9and the MPEG decoder which decrypts theseand 14 are television receivers (TV) in which the picture image data and voice data which are outputted from MPEG decoder 13 are supplied further.
[0013]This data transmitting system tends to protect packet data from an illegal copy by transmitting the standard stream for MPEG outputted from MPEG encoder 3 as a stream which carries out the scramble of the stream of a packet data division.
[0014]
[Problem(s) to be Solved by the Invention]Howeverin this data transmitting systemfor exampleit is shown in drawing 13 -- as -- as the stream of MPEG encoder 3 to a packet data division -- a1a2and a3 -- while ... is outputted -- the random number c1 from the random number generators 5 and 10c2and c3 -- the case where ... is outputted -- the output of EOR circuit 6[0015]

[Equation 1]



[0016]the stream outputted from EOR circuit 11 since a next door and this will be outputted from the selection circuitry 7 and will be inputted into EOR circuit 11 -- a1a2and a3 -- it becomes ... Thereforethe stream inputted into EOR circuit 11[0017]

[Equation 2]



[0018]the stream a1 outputted from EOR circuit 11a2and a3 -- the random number c1 which will be outputted from the random number generator 10 if EOR processing of ... is carried out in EOR circuit 15c2and c3 ... can be obtained.

[0019]Thusin this data transmitting systemeven when the key signal was unknownthere was a problem that there was a possibility of the random number pattern outputted from the random number generator 10 being copied easilyand descrambling also about the packet data by which scramble was carried out.

[0020]An object of this invention is to provide the scrambling method and device and the descrambling method of having enabled it to realize high data transmission of confidentialitya devicethe data transmission methodand a system in view of this point.

[0021]

[Means for Solving the Problem]Inside of a stream in which a scrambling method of this invention puts in a row a stream which arranged the 2nd stream part behind the 1st stream part as a unit streamIt is a scrambling method which carries out the scramble of the 2nd stream part made into an object of scramble using a random number generatorWhen said 1st data value of stream circles supplies said random number generator every 2nd stream part made into an object of said scramble by making into an initial value a data value of predetermined data which is not constantIt carries out [which scrambles the 2nd stream part made into an object of said scramble].

[0022]When using a scrambling method of this inventiondescrambling will be performed when the 1st data value of stream circles supplies a random number generator every 2nd stream part by which scramble is carried out by making into an initial value a data value of predetermined data which is not constant.

[0023]That issince an initial value which does not set a value constant will be supplied every 2nd stream part by which scramble is carried out to a random number generator by the side of descramblingit becomes difficult to analyze a random number pattern generated from a random number generatorand high data transmission of confidentiality can be realized.

[0024]Inside of a stream in which a scramble device of this invention puts in a row a stream which arranged the 2nd stream part behind the 1st stream part as a unit streamA random number generator which is a scramble device which carries out the scramble of the 2nd stream part made into an object of scrambleand

generates a random numberAn initial value supply circuit supplied to said random number generator every 2nd stream part made into an object of said scramble by making into an initial value a data value of predetermined data said 1st data value of stream circles is not constantIt has a logic operation circuit which carries out the scramble of the 2nd stream part that carries out the logical operation of the 2nd stream part made into an object of said scrambleand the random number outputted from said random number generatorand is made into an object of said scrambleand is called a preparation.

[0025]In using a scramble device of this inventionA descrambling device every 2nd stream part by which scramble is carried out to a random number generator which generates a random number. An initial value supply circuit supplied to a random number generator by making into an initial value a data value of predetermined data whose 1st data value of stream circles is not constantIt will have a logic operation circuit which descrambles the 2nd stream part by which scramble is carried out by carrying out the logical operation of the 2nd stream part by which scramble is carried outand the random number outputted from a random number generatorand will be constituted.

[0026]Namelyto a random number generator of a descrambling device. Since an initial value which does not set a value constant will be supplied every 2nd stream part by which scramble is carried outit becomes difficult to analyze a random number pattern generated from a random number generatorand high data transmission of confidentiality can be realized.

[0027]Inside of a stream in which a descrambling method of this invention puts in a row a stream which arranged the 2nd stream part behind the 1st stream part as a unit streamIt is the descrambling method which descrambles the 2nd stream part made into an object of descrambling using a random number generatorWhen said 1st data value of stream circles supplies said random number generator every 2nd stream part made into an object of said descrambling by making into an initial value a data value of predetermined data which is not constantThe 2nd stream part made into an object of said descrambling is descrambled.

[0028]According to a descrambling method of this inventionto a random number generator. Since an initial value which does not set a value constant will be supplied every 2nd stream part by which scramble is carried outit becomes difficult to analyze a random number pattern generated from a random number generatorand high data transmission of confidentiality can be realized.

[0029]Inside of a stream in which a descrambling device of this invention puts in a row a stream which arranged the 2nd stream part behind the 1st stream part as a unit streamA random number generator which is a descrambling device which descrambles the 2nd stream part made into an object of descramblingand generates a random numberAn initial value supply circuit supplied to said random number generator every 2nd stream part made into an object of said descrambling by making into an initial value a data value of predetermined data said 1st data value of stream circles is not constantIt has a logic operation circuit which descrambles the 2nd stream part that carries out the logical operation of the 2nd

stream part made into an object of said descramblingand the random number outputted from said random number generatorand is made into an object of said descrambling.
[0030]According to the descrambling device of this inventionto a random number generator. Since an initial value which does not set a value constant will be supplied every 2nd stream part by which scramble is carried outit becomes difficult to analyze a random number pattern generated from a random number generatorand high data transmission of confidentiality can be realized.
[0031]A data transmission method of this invention about a stream which puts in a row a stream which arranged the 2nd stream part behind the 1st stream part to a transmitting agency as a unit stream. Perform a scrambling method of this invention and a stream obtained by this is transmitted to a transfer place via transfer mediaA process of restoring a stream which puts in a row a stream which performed a descrambling method of ******** in a transfer placeand arranged the 2nd stream part behind the 1st stream part as a unit stream is included.
[0032]Since a scrambling method of this invention and a descrambling method of this invention are used according to a data transmission method of this inventionhigh data transmission of confidentiality is realizable.
[0033]A data transmitting system of this invention has a scramble device of this inventionTransfer origin which is changed into a stream which carries out the scramble of the 2nd stream part for which a stream which puts in a row a stream which arranged the 2nd stream part behind the 1st stream part as a unit stream is set as the object of scrambleand is transmitted to transfer mediaIt has a descrambling device of this inventionand it has a transfer place which restores a stream which arranged the 2nd stream part for a stream supplied from transfer media behind the 1st stream part to a stream put in a row as a unit streamand is constituted.
[0034]Since a scramble device of this invention and a descrambling device of this invention are used according to the data transmission device of this inventionhigh data transmission of confidentiality is realizable.
[0035]
[Embodiment of the Invention]Hereafterwith reference to drawing 1 – drawing 11the 1st gestalt of operation of the data transmission method of this invention and a system – the 5th gestalt are explained including the scrambling method of this inventiona devicethe descrambling method of this inventionand the embodiment of a device.
[0036]The 1st gestalt .. Drawing 1 – drawing 4 drawing 1 are the block diagrams showing the important section of the data transmitting system (the 1st gestalt of operation of the data transmitting system of this invention) used for operation of the 1st gestalt of implementation of the data transmission method of this invention.
[0037]A microphone for a camera for 20 to obtain picture image data among drawing 1 and 21 to obtain voice data22 is an MPEG encoder which codes and carries out Time Division Multiplexing of the picture image data obtained with the camera 20and the voice data obtained with the microphone 21and is encoded to

the stream based on an MPEG 2-PS (program stream) standard.
[0038]Drawing 2 is a figure showing the structure of the PES (Packetized Elementary Stream) packet of MPEG 2-PS. Among drawing 2PTS (Presentation Time Stamp) is the time-of-day-control information on a reproducing outputandgenerally is inserted every 700 ms.
[0039]It is a flag with which DTS (Decoding Time Stamp) shows whetheras for the data in which the time-of-day-control information on decoding and PES scramble control display the existence of scramble controland a PTS&DTS flagPTS data exists.
[0040]In drawing 123 is a scramble circuit where the stream of the packet data division made into the object of scramble changes the stream outputted from MPEG encoder 22 into the stream which comes to carry out scramble.
[0041]This scramble circuit 23 is a scramble device used for operation of the 1st gestalt of operation of the scrambling method of this inventionand makes the 1st gestalt of operation of the scramble device of this invention.
[0042]The random number generator of a DES (Data Encryption Standard) standard which generates the random number of the series as which 24 is specified by a key signal in the scramble circuit 2325 is a position detecting circuit which inputs the stream outputted from MPEG encoder 22and performs detection of a packet start codethe check of the contents of PES scramble controlthe check of a PTS&DTS flagthe detecting position of PTSstarting position detection of a packet data divisionetc.
[0043]26 is a data holding circuit holding PTS dataand this data holding circuit 26 will be controlled by the position detecting circuit 25 to hold the data of this PTS that carried out the detecting positionif the position detecting circuit 25 detects the position of PTS.
[0044]27 is the random number itself outputted from the PTS data or the random number generator 24 which the data holding circuit 26 holds a selection circuitry supplied to the random number generator 24and this selection circuitry 27If the position detecting circuit 25 detects the starting position of the packet data division made into the object of scrambleIt is controlled by the position detecting circuit 25 to feed back the random number outputted from the random number generator 24 until it supplies the random number generator 24 by making into an initial value the PTS data which the data holding circuit 26 holds and the stream of a packet data division is completed after that.
[0045]The initial value supply circuit in the scramble circuit 23 comprises these position detecting circuits 25the data holding circuit 26and the selection circuitry 27.
[0046]The inside of the stream to which 28 is outputted from MPEG encoder 22It is an EOR circuit which carries out the scramble of the stream of the packet data division which carries out EOR processing of the stream of the packet data division made into the object of scrambleand the random number outputted from the random number generator 24and is made into the object of scramble.
[0047]Chooseand 29 is the stream outputted from MPEG encoder 22and the

stream outputted from EOR circuit 28 a selection circuitry to outputand this selection circuitry 29It is controlled by the position detecting circuit 25 to output the stream from which the stream of the packet data division made into the object of scramble changed the stream outputted from MPEG encoder 22 into the stream which comes to carry out scramble.

[0048]Storage mediasuch as a disk with which 30 accumulates the stream outputted from the selection circuitry 29i.e.the stream outputted from the scramble circuit 2331 is a descramble circuit where the stream of the packet data division by which scramble is carried out changes the stream supplied from the storage medium 30 into the stream which it comes to descramble.

[0049]This descramble circuit 31 is a descrambling device used for operation of the 1st gestalt of implementation of the descrambling method of this inventionand makes the 1st gestalt of operation of the descrambling device of this invention.

[0050]In this descramble circuit 3132 is a random number generator of the same circuitry as the random number generator 24and the key signal and the key signal of an identical content which were used for the random number generator 24 are supplied to this random number generator 32.

[0051]33 is a position detecting circuit which inputs the stream supplied from the storage medium 30and performs detection of a packet start codethe check of the contents of PES scramble controlthe check of a PTS&DTS flagthe detecting position of PTSstarting position detection of a packet data divisionetc.

[0052]34 is a data holding circuit holding PTS dataand this data holding circuit 34 will be controlled by the position detecting circuit 33 to hold the data of this PTS that carried out the detecting positionif the position detecting circuit 33 detects the position of PTS.

[0053]35 is the random number itself outputted from the PTS data or the random number generator 32 which the data holding circuit 34 holds a selection circuitry supplied to the random number generator 32and this selection circuitry 35If the position detecting circuit 33 detects the object of descramblingi.e.the starting position of a packet data division by which scramble is carried outIt is controlled by the position detecting circuit 33 to feed back the random number outputted from the random number generator 32 until it supplies the random number generator 32 by making into an initial value the PTS data which the data holding circuit 34 holds and the stream of a packet data division is completed after that.

[0054]The initial value supply circuit in the descramble circuit 31 comprises these position detecting circuits 33the data holding circuit 34and the selection circuitry 35.

[0055]36 carries out EOR processing of the stream of the packet data division by which scramble is carried out among the streams supplied from the storage medium 30and the random number outputted from the random number generator 32It is an EOR circuit which descrambles the stream of the packet data division by which scramble is carried out.

[0056]Chooseand 37 is the stream supplied from the storage medium 30and the stream outputted from EOR circuit 36 a selection circuitry to outputand this

selection circuitry 37It is controlled by the position detecting circuit 33 to output the stream which changed the stream supplied from the storage medium 30 into the stream which comes to descramble the stream of the packet data division by which scramble is carried out.

[0057]The MPEG decoder which 38 separates the stream of picture image dataand the stream of voice data from the stream outputted from the selection circuitry 37i.e.the stream outputted from the descramble circuit 31and is decrypted39 is a television receiver in which the picture image data and voice data which are outputted from MPEG decoder 38 are supplied.

[0058]In this data transmitting systemthe picture image data obtained with the camera 20and the voice data obtained with the microphone 21By MPEG encoder 22it is encoded by the stream based on an MPEG 2-PS standardand is inputted into the scramble circuit 23and the position detecting circuit 25the data holding circuit 26EOR circuit 28and the selection circuitry 29 are supplied.

[0059]In [drawing 3 is a flow chart for explaining operation (the 1st gestalt of operation of the scrambling method of this invention) of the scramble circuit 23and] the scramble circuit 23Since the same operation is performed repeatedlyand the output of the stream of a packet data division made into the object of scramble from the selection circuitry 29 was endedif operation is explainedThe position detecting circuit 25 controls the selection circuitry 29 to continue outputting the stream inputted from MPEG encoder 22 as it is (Step S1)and will be in the state for detecting a packet start code (Step S2).

[0060]And when the position detecting circuit 25 detects a packet start codeIt is judged from the contents of scramble control of a packet header unit whether the stream of a packet data division is an object of scramble (Step S3)When not considered as the object of scramble (in the case of NO)operation returns to Step S2 and the position detecting circuit 25 will be in the state for detecting a packet start code.

[0061]On the other handwhen the stream of the packet data division is made into the object of scramble (in the case [Setting to Step S3.] of YES). The position detecting circuit 25 judges the existence of whether the PTS&DTS flag of a packet header unit is "10" or "11"and PTS data (step S4).

[0062]When a PTS&DTS flag is "10" or "11" as a result of judgment (i.e.when PTS data exists)The position detecting circuit 25 detects the position of PTSmakes PTS data hold to the data holding circuit 26 (Step S5)and will be in the state for detecting the starting position of a packet data division (Step S6).

[0063]On the other handwhen a PTS&DTS flag is except "10" or "11" (i.e.when PTS data does not exist)the position detecting circuit 25 will be in the state for detecting the starting position of a packet data division as it is (Step S6).

[0064]And if the starting position of a packet data division is detectedthe position detecting circuit 25The PTS data which the data holding circuit 26 holdsi.e.the same data of PTS of the packet header unit of a packet as the packet data division which is going to carry out scrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which is going

to carry out scramble. The selection circuitry 27 is controlled to supply the random number generator 24 among the packet header units in which PTS exists by making the PTS data of the last packet header unit into an initial value (Step S7).

[0065]The stream of the packet data division made into the object of scramble among the streams outputted here from MPEG encoder 22 in EOR circuit 28EOR processing of the random number outputted from the random number generator 24 is carried outand the scramble of the stream of the packet data division made into the object of scramble is performed.

[0066]Thenthe position detecting circuit 25 controls the selection circuitry 29makes it continue outputting the stream which is outputted from EOR circuit 28 and by which scramble was carried out (Step S8)and it returns to waiting (step S9) and Step S1 until the stream of a packet data division is completed.

[0067]Thusthe stream outputted from MPEG encoder 22The stream which the stream of the packet data division made into the object of scramble was changed into the stream which comes to carry out scramblewas accumulated in the storage medium 30and was accumulated in this storage medium 30 will be suitably supplied to the descramble circuit 31.

[0068]In [drawing 4 is a flow chart for explaining operation (the 1st gestalt of implementation of the descrambling method of this invention) of the descramble circuit 31and] the descramble circuit 31Since the same operation is performed repeatedlyand the output of the stream of a packet data division made into the object of descrambling from the selection circuitry 37 was endedif operation is explainedThe position detecting circuit 33 controls the selection circuitry 37 to continue outputting the stream supplied from the storage medium 30 as it is (Step P1)and will be in the state for detecting a packet start code (Step P2).

[0069]And when the position detecting circuit 33 detects a packet start code. [whether the stream of the packet data division is made into the object of descrambling from the contents of scramble control of a packet header unitand] Namelyit judges whether scramble is carried out (Step P3)and when scramble is not carried out (in the case of NO)operation returns to Step P2 and the position detecting circuit 33 will be in the state for detecting a packet start code.

[0070]On the other handwhen the scramble of the stream of a packet data division is carried out (in the case [Setting to Step P3.] of YES). The position detecting circuit 33 judges the existence of whether the PTS&DTS flag of a packet header unit is "10" or "11"and PTS data (Step P4).

[0071]When a PTS&DTS flag is "10" or "11" as a result of judgment (i.e.when PTS data exists)The position detecting circuit 33 detects the position of PTSmakes PTS data hold to the data holding circuit 34 (Step P5)and will be in the state for detecting the starting position of a packet data division (Step P6).

[0072]On the other handwhen a PTS&DTS flag is except "10" or "11" (i.e.when PTS data does not exist)the position detecting circuit 33 will be in the state for detecting the starting position of a packet data division as it is (Step P6).

[0073]And if the starting position of a packet data division is detectedthe position

detecting circuit 33The PTS data which the data holding circuit 34 holdsi.e.the same data of PTS of the packet header unit of a packet as the packet data division which it is going to descrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which it is going to descramble. The selection circuitry 35 is controlled to supply the random number generator 32 among the packet header units in which PTS exists by making the PTS data of the last packet header unit into an initial value (Step P7).

[0074]The stream of the packet data division by which scramble is carried out among the streams supplied here from the storage medium 30 in EOR circuit 36EOR processing of the random number outputted from the random number generator 32 is carried outand descrambling of the stream of the packet data division by which scramble is carried out is performed.

[0075]Thenthe position detecting circuit 33 controls the selection circuitry 37makes it continue outputting the descrambled stream which is outputted from EOR circuit 36 (Step P8)and it returns to waiting (Step P9) and Step P1 until the stream of a packet data division is completed.

[0076]Thusthe stream of the packet data division by which scramble is carried out is changed into the stream which it comes to descrambleand the stream supplied from the storage medium 30 is transmitted to MPEG decoder 38.

[0077]In MPEG decoder 38the stream of picture image data and the stream of voice data are separated from the stream transmitted from the descramble circuit 31it is decrypted and the picture image data and voice data which were these-decrypted are transmitted to the television receiver 39.

[0078]Thusin the data transmission method of this inventionand the 1st gestalt of operation of a systemThe standard stream for MPEG 2-PS outputted from MPEG encoder 22It is changed into the stream which carries out the scramble of the stream of the packet data division made into the object of scramble in the scramble circuit 23and via the storage medium 30The descramble circuit 31 is suppliedescrambling is performed and it is transmitted to MPEG decoder 38.

[0079]For every stream of the packet data division made into the object of scramble in the scramble circuit 23 here. The same data of PTS of the packet header unit of a packet as the packet data division which is going to carry out scrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which is going to carry out scramble. The scramble of the stream of the packet data division made into the object of scramble is performed by supplying the random number generator 24 among the packet header units in which PTS exists by making the data value of PTS of the last packet header unit into an initial value.

[0080]As a resultin the descramble circuit 31The same data of PTS of the packet header unit of a packet as the packet data division which it is going to descramble for every stream of the packet data division by which scramble is carried outOr when PTS does not exist in the packet header unit of the same packet as the packet data division which it is going to descramble. Descrambling of the stream of the packet data division by which scramble is carried out will be performed by

supplying the random number generator 32 among the packet header units in which PTS exists by making the data value of PTS of the last packet header unit into an initial value.
[0081]Thusaccording to the data transmission method of this inventionand the 1st gestalt of operation of a systemto the random number generator 32 of the descramble circuit 31. Since the data value of PTS which does not set a data value constant will be supplied as an initial value for every stream of the packet data division by which scramble is carried outIt becomes difficult to analyze the random number pattern generated from the random number generator 32and high data transmission of confidentiality can be realized.
[0082]The 2nd gestalt .. Drawing 5 - drawing 8 drawing 5 are the block diagrams showing the important section of the data transmitting system (the 2nd gestalt of operation of the data transmitting system of this invention) used for operation of the 2nd gestalt of implementation of the data transmission method of this invention.
[0083]A microphone for a camera for 41 to obtain picture image data among drawing 5 and 42 to obtain voice data43 is an MPEG encoder which codes and carries out Time Division Multiplexing of the picture image data obtained with the camera 41and the voice data obtained with the microphone 42and is encoded to the stream based on an MPEG 2-TS (transport stream) standard.
[0084]In [drawing 6 is a figure showing the structure of the transport packet of MPEG 2-TSand] an MPEG decoder PCR (Program Clock Reference)It is the information for setting and proofreading the value of STC (basic synchronized signal) used as a time standard at the value intended with MPEG encoder 43. Generally PCR is inserted every 100 ms.
[0085]They are a flag with which an adaptation flag shows the existence of the adaptation fielda flag with which a pay-load flag shows the existence of a pay loadand a flag which shows whether an PCR flag has PCR.
[0086]In drawing 544 is a scramble circuit where the stream of the payload part made into the object of scramble changes the stream outputted from MPEG encoder 43 into the stream which comes to carry out scramble.
[0087]This scramble circuit 44 is a scramble device used for operation of the 2nd gestalt of operation of the scrambling method of this inventionand makes the 2nd gestalt of operation of the scramble device of this invention.
[0088]The random number generator of a DES standard which generates the random number of the series as which 45 is specified by a key signal in the scramble circuit 44The detection of a synchronous byte included in the stream to which 46 is outputted from MPEG encoder 43It is a position detecting circuit which performs the check of the contents of the adaptation flagthe check of the contents of the pay-load flagthe check of the contents of the PCR flagthe detecting position of PCRstarting position detection of a payload partetc.
[0089]47 is a data holding circuit holding PCR dataand this data holding circuit 47 will be controlled by the position detecting circuit 46 to hold the data of this PCR that carried out the detecting positionif the position detecting circuit 46 detects

the position of PCR.
[0090]48 is the random number itself outputted from the PCR data or the random number generator 45 which the data holding circuit 47 holds a selection circuitry supplied to the random number generator 45and this selection circuitry 48Until it will supply the random number generator 45 by making into an initial value the PCR data which the data holding circuit 47 holds and the stream of a payload part will be completed after thatif the position detecting circuit 46 detects the starting position of the payload part of the object of scrambleIt is controlled by the position detecting circuit 46 to feed back the random number outputted from the random number generator 45.
[0091]The initial value supply circuit in the scramble circuit 44 comprises these position detecting circuits 46the data holding circuit 47and the selection circuitry 48.
[0092]The inside of the stream to which 49 is outputted from MPEG encoder 43It is an EOR circuit which carries out the scramble of the stream of the payload part which carries out EOR processing of the stream of the payload part made into the object of scrambleand the random number outputted from the random number generator 45and is made into the object of scramble.
[0093]Chooseand 50 is the stream outputted from MPEG encoder 43and the stream outputted from EOR circuit 49 a selection circuitry to outputand this selection circuitry 50It is controlled by the position detecting circuit 46 to output the stream from which the stream of the payload part made into the object of scramble changed the stream outputted from MPEG encoder 43 into the stream which comes to carry out scramble.
[0094]An up converter for the digital modulation machine with which 51 carries out digital modulation of the stream outputted from the selection circuitry 50i.e.the stream outputted from the scramble circuit 44and 52 to transmit the output of the digital modulation machine 51and 53 are the antennas of the transmitting side.
[0095]The tuner with which 54 performs the antenna of a receiver and 55 tunes inand 56 are digital demodulation machines which carry out digital demodulation of the signal tuned in with the tuner 55.
[0096]57 is a descramble circuit changed into the stream which descrambled the stream of the payload part by which scramble is carried out in the stream outputted from the digital demodulation machine 56.
[0097]This descramble circuit 57 is a descrambling device used for operation of the 2nd gestalt of implementation of the descrambling method of this inventionand makes the 2nd gestalt of operation of the descrambling device of this invention.
[0098]In the descramble circuit 5758 is a random number generator of the same circuitry as the random number generator 45and the key signal and the key signal of an identical content which were used for the random number generator 45 are supplied to this random number generator 58.
[0099]The detection of a synchronous byte included in the stream to which 59 is outputted from the digital demodulation machine 56It is a position detecting circuit which performs the check of the contents of the adaptation flagthe check of the

contents of the pay-load flagthe check of the contents of the PCR flagthe detecting position of PCRstarting position detection of a payload partetc.
[0100]60 is a data holding circuit holding PCR dataand this data holding circuit 60 will be controlled by the position detecting circuit 59 to hold the data of this PCR that carried out the detecting positionif the position detecting circuit 59 detects the position of PCR.
[0101]61 is the random number itself outputted from the PCR data or the random number generator 58 which the data holding circuit 60 holds a selection circuitry supplied to the random number generator 58and this selection circuitry 61If the position detecting circuit 59 detects the object of descramblingi.e.the position of a payload part by which scramble is carried outIt is controlled by the position detecting circuit 59 to feed back the random number outputted from the random number generator 58 until it supplies the random number generator 58 by making into an initial value the PCR data which the data holding circuit 60 holds and the stream of a payload part is completed after that.
[0102]The initial value supply circuit in the descramble circuit 57 comprises these position detecting circuits 59the data holding circuit 60and the selection circuitry 61.
[0103]62 is an EOR circuit which carries out EOR processing of the stream of the payload part by which scramble is carried out among the streams inputted from the digital demodulation machine 56and the random number outputted from the random number generator 58and descrambles the stream of the payload part by which scramble is carried out.
[0104]Chooseand 63 is the stream outputted from the digital demodulation machine 56and the stream outputted from EOR circuit 62 a selection circuitry to outputand this selection circuitry 63It is controlled by the position detecting circuit 59 to output the stream which changed the stream outputted from the digital demodulation machine 56 into the stream which comes to descramble the stream of the payload part by which scramble is carried out.
[0105]The MPEG decoder which 64 separates the stream of picture image dataand the stream of voice data from the stream outputted from the selection circuitry 63i.e.the stream outputted from the descramble circuit 57and is decrypted65 is a television receiver in which the picture image data and voice data which are outputted from MPEG decoder 64 are supplied.
[0106]In this data transmitting systemthe picture image data obtained with the camera 41and the voice data obtained with the microphone 42By MPEG encoder 43it is encoded by the stream based on an MPEG 2-TS standardand is inputted into the scramble circuit 44and the position detecting circuit 46the data holding circuit 47EOR circuit 49and the selection circuitry 50 are supplied.
[0107]In [drawing 7 is a flow chart for explaining operation (the 2nd gestalt of operation of the scrambling method of this invention) of the scramble circuit 44and] the scramble circuit 44Since the same operation is performed repeatedlyand the output of the stream of a payload part made into the object of scramble from the selection circuitry 50 was endedif operation is explainedThe

position detecting circuit 46 controls the selection circuitry 50 to continue outputting the stream inputted from MPEG encoder 43 as it isand will be in the state for detecting a synchronous byte (Step N1).
[0108]And the position detecting circuit 46 judges whether the stream of the payload part is made into the object of scramble from the contents of scramble control of a packet header unitwhen a synchronous byte is detected (Step N2)When not considered as the object of scramble (in the case of NO)operation returns to Step N1 and the position detecting circuit 46 will be in the state for detecting a synchronous byte.
[0109]On the other handwhen the stream of the payload part is made into the object of scramble (in the case [Setting to Step N3.] of YES)the position detecting circuit 46 judges whether there is any adaptation field from an adaptation flag (Step N3).
[0110]When there is the adaptation field as a result of judgment (when it is YES)When it judges whether the position detecting circuit 46 has PCR from an PCR flag (Step N4) and there is PCRthe position of PCR is detected (when it is YES)and PCR data is made to hold to the data holding circuit 47 (Step N5).
[0111]And when it judges whether the position detecting circuit 46 has a pay load from a pay-load flag (Step N6) and there is a pay load (when it is YES). When there are not waiting (Step N7) and a pay load until it detects the starting position of a payload partoperation returns to Step N1 (when it is NO).
[0112]When it judged that there was no adaptation field here in Step N3or when it is judged that there is no PCR in Step N4 (when it is NO)operation shifts to Step N6 (when it is NO).
[0113]And after Step N7 and the position detecting circuit 46The PCR data which the data holding circuit 47 will hold if the starting position of a payload part is detectedNamelythe data of the same PCR of the packet header unit of a packet as the payload part which is going to carry out scrambleOr when PCR does not exist in the packet header unit of the same packet as the payload part which is going to carry out scramble. The selection circuitry 48 is controlled to supply the random number generator 45 among the packet header units in which PCR exists by making the PCR data of the last packet header unit into an initial value (Step N8).
[0114]The stream of the payload part made into the object of scramble among the streams inputted here from MPEG encoder 43 in EOR circuit 49EOR processing of the random number outputted from the random number generator 45 is carried outand the scramble of the payload part made into the object of scramble is performed.
[0115]And the position detecting circuit 46 controls the selection circuitry 50makes it continue outputting the stream which is outputted from EOR circuit 49 and by which scramble was carried out (Step N9)and it returns to waiting (Step N10) and Step N1 until the stream of a payload part is completed.
[0116]Thusthe stream outputted from MPEG encoder 43The stream of the payload part made into the object of scramble is changed into the stream which

comes to carry out scrambleand is transmitted to the descramble circuit 57 via the digital modulation machine 51the up converter 52the antennas 53 and 54the tuner 55and the digital demodulation machine 56.
[0117]In [drawing 8 is a flow chart for explaining operation (the 2nd gestalt of implementation of the descrambling method of this invention) of the descramble circuit 57and] the descramble circuit 57Since the same operation is performed repeatedlyand the output of the stream of the payload part made into the object of descrambling from the selection circuitry 63i.e.the payload part by which scramble is carried outwas endedif operation is explainedThe position detecting circuit 59 controls the selection circuitry 63 to continue outputting the stream inputted from the digital demodulation machine 56 as it isand will be in the state for detecting a synchronous byte (Step Q1).
[0118]When a synchronous byte is detectedthe stream of a payload part the position detecting circuit 59 from the contents of scramble control of a packet header unit And the object of descramblingNamelyit judges whether scramble is carried out (Step Q2)and when scramble is not carried out (in the case of NO)operation returns to Step Q1 and the position detecting circuit 46 will be in the state for detecting a synchronous byte.
[0119]On the other handwhen the stream of the payload part is made into the object of scramble (in the case [Setting to Step Q2.] of YES)the position detecting circuit 59 judges whether there is any adaptation field from an adaptation flag (Step Q3).
[0120]When there is the adaptation field as a result of judgment (when it is YES)When it judges whether the position detecting circuit 59 has PCR from an PCR flag (Step Q4) and there is PCRthe position of PCR is detected (when it is YES)and PCR data is made to hold to the data holding circuit 60 (Step Q5).
[0121]And when it judges whether the position detecting circuit 59 has a pay load from a pay-load flag (Step Q6) and there is a pay load (when it is YES). When there are not waiting (Step Q7) and a pay load until it detects the starting position of a payload partoperation returns to Step Q1 (when it is NO).
[0122]When it judged that there was no adaptation field here in Step Q3or when it is judged that there is no PCR in Step Q4 (when it is NO)operation shifts to Step Q6 (when it is NO).
[0123]And after Step Q7 and the position detecting circuit 59The PCR data which the data holding circuit 60 will hold if the starting position of a payload part is detectedNamelythe data of the same PCR of the packet header unit of a packet as the payload part which it is going to descrambleOr when PCR does not exist in the packet header unit of the same packet as the payload part which it is going to descramble. The selection circuitry 61 is controlled to supply the random number generator 58 among the packet header units in which PCR exists by making the PCR data of the last packet header unit into an initial value (Step Q8).
[0124]EOR processing of the stream of the payload part by which scramble is carried out among the streams inputted here from the digital demodulation machine 56 in EOR circuit 62and the random number outputted from the random

number generator 58 is carried outand descrambling of the payload part by which scramble is carried out is performed.
[0125]And the position detecting circuit 59 controls the selection circuitry 63makes it continue outputting the descrambled stream which is outputted from EOR circuit 62 (Step Q9)and it returns to waiting (Step Q10) and Step Q1 until the stream of a payload part is completed.
[0126]Thusin the descramble circuit 57the stream of the payload part by which scramble is carried out is changed into the stream which it comes to descrambleand the stream outputted from the digital demodulation machine 56 is transmitted to MPEG decoder 64.
[0127]In MPEG decoder 64the stream of picture image data and the stream of voice data are separated from the stream transmitted from the descramble circuit 57it is decrypted and the picture image data and voice data which were these-decrypted are transmitted to the television receiver 65.
[0128]Thusin the data transmission method of this inventionand the 2nd gestalt of operation of a systemThe standard stream for MPEG 2-TS outputted from MPEG encoder 43In the scramble circuit 44it is changed into the stream which carries out the scramble of the stream of the payload part made into the object of scramblethe descramble circuit 57 is supplieddescrambling is performedand it is transmitted to MPEG decoder 64.
[0129]For every stream of the payload part made into the object of scramble in the scramble circuit 44 here. The data of the same PCR of the packet header unit of a packet as the payload part which is going to carry out scrambleOr when PCR does not exist in the packet header unit of the same packet as the payload part which is going to carry out scramble. The scramble of the stream of the payload part made into the object of scramble is performed by supplying the random number generator 45 among the packet header units in which PCR exists by making the data value of PCR of the last packet header unit into an initial value.
[0130]As a resultin the descramble circuit 57The data of the same PCR of the packet header unit of a packet as the payload part which it is going to descramble for every stream of the payload part by which scramble is carried outOr when PCR does not exist in the packet header unit of the same packet as the payload part which it is going to descramble. Descrambling of the stream of the payload part by which scramble is carried out will be performed by supplying the random number generator 58 among the packet header units in which PCR exists by making the data value of PCR of the last packet header unit into an initial value.
[0131]Thusaccording to the data transmission method of this inventionand the 2nd gestalt of operation of a systemto the random number generator 58 of the descramble circuit 57. Since the data value of PCR which does not set a data value constant will be supplied as an initial value for every stream of the payload part by which scramble is carried outit becomes difficult to analyze the random number pattern generated from the random number generator 58and high data transmission of confidentiality can be realized.
[0132]Although this example explained the case where it was made to supply the

random number generators 45 and 58 by making the data value of PCR into an initial valueIt may be made to instead supply combination or the calculated data value of data for the data value of a round counter or PCRand a round counter at the random number generators 45 and 58for example.
[0133]The 3rd gestalt .. Drawing 9 drawing 9 is a block diagram showing the important section of the data transmitting system (the 3rd gestalt of operation of the data transmitting system of this invention) used for operation of the 3rd gestalt of implementation of the data transmission method of this invention.
[0134]A microphone for a camera for 67 to obtain picture image data among drawing 9 and 68 to obtain voice data69 is an MPEG encoder which codes and carries out Time Division Multiplexing of the picture image data obtained with the camera 67and the voice data obtained with the microphone 68and is encoded to the stream based on an MPEG 2-PS standard.
[0135]70 is a scramble circuit where the stream of the packet data division made into the object of scramble changes the stream outputted from MPEG encoder 69 into the stream which comes to carry out scramble.
[0136]This scramble circuit 70 is a scramble device used for operation of the 3rd gestalt of operation of the scrambling method of this inventionand makes the 3rd gestalt of operation of the scramble device of this invention.
[0137]The random number generator of a DES standard which generates the random number of the series as which 71 is specified by a key signal in the scramble circuit 7072 is a position detecting circuit which inputs the stream inputted from MPEG encoder 69and performs detection of a packet start codethe check of the contents of PES scramble controlthe check of the contents of the PTS&DTS flagthe detecting position of PTSstarting position detection of a packet data divisionetc.
[0138]The serial/parallel-conversion circuit (S/P) where 73 carries out parallel conversion of the stream inputted from MPEG encoder 69 to a 64-bit parallel stream74 is a register (RS) of 40 bit configurations holding PTS dataand this register 74 will be controlled by the position detecting circuit 72 to hold the PTS data outputted from the serial/parallel-conversion circuit 73if the position detecting circuit 72 detects the position of PTS.
[0139]75 is a register of 64 bit configurations holding the stream of the packet data division made into the object of scramble among the streams which are controlled by the position detecting circuit 72 and outputted from the serial/parallel-conversion circuit 73.
[0140]76 is the random number itself outputted from the PTS data or the random number generator 71 which the register 74 holds a selection circuitry supplied to the random number generator 71and this selection circuitry 76If the position detecting circuit 72 detects the starting position of the packet data division made into the object of scrambleIt is controlled by the position detecting circuit 72 to feed back the random number outputted from the random number generator 71 until it supplies the random number generator 71 by making into an initial value the PTS data which the register 74 holds and the stream of a packet data division is

completed after that.
[0141]The initial value supply circuit in the scramble circuit 70 comprises the position detecting circuit 72the register 74and the selection circuitry 76.
[0142]77 is an EOR circuit which carries out the scramble of the stream of the packet data division which carries out EOR processing of the stream of the parallel stream outputted from the register 75and the random number outputted from the random number generator 71and is made into the object of scramble.
[0143]The register of 64 bit configurations holding the parallel stream which 78 is controlled by the position detecting circuit 72 and outputted from EOR circuit 77and 79 are parallel/serial-conversion circuits (P/S) which carry out serial conversion of the parallel stream outputted from the register 78.
[0144]80 is a selection circuitry which chooses and outputs the stream inputted from MPEG encoder 69and the stream outputted from parallel / SHISHIARU conversion circuit 79This selection circuitry 80 is controlled by the position detecting circuit 72 to output the stream from which the stream of the packet data division made into the object of scramble changed the stream inputted from MPEG encoder 69 into the stream which comes to carry out scramble.
[0145]Storage mediasuch as a disk with which 81 accumulates the stream outputted from the selection circuitry 80i.e.the stream outputted from the scramble circuit 7082 is a descramble circuit changed into the stream which descrambled the stream of the packet data division by which scramble is carried out in the stream supplied from the storage medium 81.
[0146]This descramble circuit 82 is a descrambling device used for operation of the 3rd gestalt of implementation of the descrambling method of this inventionand makes the 3rd gestalt of operation of the descrambling device of this invention.
[0147]In the descramble circuit 8283 is a random number generator of the same circuitry as the random number generator 71and the key signal and the key signal of an identical content which were used for the random number generator 71 are supplied to this random number generator 83.
[0148]84 is a position detecting circuit which inputs the stream supplied from the storage medium 81and performs detection of a packet start codethe check of the contents of PES scramble controlthe check of the contents of the PTS&DTS flagthe detecting position of PTSstarting position detection of a packet data divisionetc.
[0149]The serial/parallel-conversion circuit where 85 carries out parallel conversion of the stream supplied from the storage medium 81 to a 64-bit parallel stream86 is a register of 40 bit configurations holding PTS dataand this register 86 will be controlled by the position detecting circuit 84 to hold the PTS data outputted from the serial/parallel-conversion circuit 85if the position detecting circuit 84 detects the position of PTS.
[0150]87 is a register of 64 bit configurations holding the stream of the packet data division which is controlled by the position detecting circuit 84 and outputted from the serial/parallel-conversion circuit 85 and by which scramble is carried out.
[0151]88 is the random number itself outputted from the PTS data or the random

number generator 83 which the register 86 holds a selection circuitry supplied to the random number generator 83and this selection circuitry 88If the position detecting circuit 84 detects the object of descramblingi.e.the starting position of a packet data division by which scramble is carried outIt is controlled by the position detecting circuit 84 to feed back the random number outputted from the random number generator 83 until it supplies the random number generator 83 by making into an initial value the PTS data which the register 86 holds and the stream of a packet data division is completed after that.

[0152]The initial value supply circuit in the descramble circuit 82 comprises the position detecting circuit 84the register 86and the selection circuitry 88.

[0153]89 is an EOR circuit which carries out EOR processing of the parallel stream outputted from the register 87and the random number outputted from the random number generator 83and descrambles the stream of the packet data division by which scramble is carried out.

[0154]The register of 64 bit configurations holding the parallel stream which 90 is controlled by the position detecting circuit 84 and outputted from EOR circuit 89and 91 are parallel/serial-conversion circuits which carry out serial conversion of the parallel stream outputted from the register 90.

[0155]92 is a selection circuitry which chooses and outputs the stream supplied from the storage medium 81and the stream outputted from the parallel/serial-conversion circuit 91This selection circuitry 92 is controlled by the position detecting circuit 84 to output the stream which changed the stream supplied from the storage medium 81 into the stream which comes to descramble the stream of the packet data division by which scramble is carried out.

[0156]The MPEG decoder which 93 separates the stream of picture image dataand the stream of voice data from the stream outputted from the descramble circuit 82and is decrypted94 is a television receiver in which the picture image data and voice data which are outputted from MPEG decoder 93 are supplied.

[0157]In this data transmitting systemthe picture image data obtained with the camera 67and the voice data obtained with the microphone 68By MPEG encoder 69it is encoded by the stream based on an MPEG 2-PS standardand is inputted into the scramble circuit 70and the position detecting circuit 72the serial/parallel-conversion circuit 73and the selection circuitry 80 are supplied.

[0158]When the position detecting circuit 72 detects a packet start code hereWhen it judges whether the stream of a packet data division is an object of scramble from the contents of scramble control of a packet header unit and is not considered as the object of scrambleit returns to the state for detecting a packet start code.

[0159]On the other handwhen the stream of the packet data division is made into the object of scramblethe position detecting circuit 72 judges the existence of whether the PTS&DTS flag of a packet header unit is "10" or "11"and PTS.

[0160]When a PTS&DTS flag is "10" or "11" as a result of judgment (i.e.when PTS exists)the position detecting circuit 72 detects the position of PTSmakes PTS data hold to the register 74and will be in the state for detecting the starting

position of a packet data division.
[0161]On the other handwhen a PTS&DTS flag is except "10" or "11" (i.e.when PTS does not exist)the position detecting circuit 72 will be in the state for detecting the starting position of a packet data division as it is.
[0162]And if the starting position of a packet data division is detectedthe position detecting circuit 72The PTS data which the register 74 holdsi.e.the same data of PTS of the packet header unit of a packet as the packet data division which is going to carry out scrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which is going to carry out scramble. The selection circuitry 76 is controlled to supply the random number generator 71 among the packet header units in which PTS exists by making the PTS data of the last packet header unit into an initial valueand the stream outputted from the serial/parallel-conversion circuit 73 is made to hold to the register 75.
[0163]EOR processing of the stream outputted here from the register 75 in EOR circuit 77 and the random number outputted from the random number generator 71 is carried outThe scramble of the stream of the packet data division made into the object of scramble is performedthe result is held at the register 78and serial conversion of the parallel stream outputted from the register 78 is further carried out by the parallel/serial-conversion circuit 79.
[0164]The position detecting circuit 72 controls the selection circuitry 80and it is made to continue outputting the stream outputted from the parallel/serial-conversion circuit 79The selection circuitry 80 is controlled to output the stream inputted from waiting and MPEG encoder 69 as it is until the stream of a packet data division is completed.
[0165]Thusthe stream of the packet data division made into the object of scramble is changed into the stream which comes to carry out scrambleand the stream outputted from MPEG encoder 69 is accumulated in the storage medium 81.
[0166]And suitablythe stream accumulated in the storage medium 81 is supplied to the descramble circuit 82and is supplied to the position detecting circuit 84the serial/parallel-conversion circuit 85and the selection circuitry 92.
[0167]When the position detecting circuit 84 detects a packet start code hereWheni.e.judge whether scramble is carried outand scramble is not carried out from the contents of scramble control of a packet header unitit returns to the state for detecting a packet start code. [the object / the stream of a packet data division / of descrambling]
[0168]On the other handwhen the scramble of the stream of a packet data division is carried outthe position detecting circuit 84 judges the existence of whether the PTS&DTS flag of a packet header unit is "10" or "11"and PTS.
[0169]When a PTS&DTS flag is "10" or "11" as a result of judgment (i.e.when PTS exists)the position detecting circuit 84 detects the position of PTSmakes PTS data hold to the register 86and will be in the state for detecting the starting position of a packet data division.

[0170]On the other handwhen a PTS&DTS flag is except "10" or "11" (i.e.when PTS does not exist)the position detecting circuit 84 will be in the state for detecting the starting position of a packet data division as it is.
[0171]And if the starting position of a packet data division is detectedthe position detecting circuit 84The PTS data which the register 86 holdsi.e.the same data of PTS of the packet header unit of a packet as the packet data division which it is going to descrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which it is going to descramble. The selection circuitry 88 is controlled to supply the random number generator 83 among the packet header units in which PTS exists by making the PTS data of the last packet header unit into an initial valueand the stream outputted from the serial/parallel-conversion circuit 85 is made to hold to the register 87.
[0172]EOR processing of the stream outputted here from the register 87 in EOR circuit 89 and the random number outputted from the random number generator 83 is carried outThe scramble of the stream of the packet data division by which scramble is carried out is performedthe result is held at the register 90and serial conversion of the parallel stream outputted from the register 90 is further carried out by the parallel/serial-conversion circuit 91.
[0173]The position detecting circuit 84 controls the selection circuitry 92and it is made to continue outputting the stream outputted from the parallel/serial-conversion circuit 91The selection circuitry 92 is controlled to output the stream supplied from the storage medium 81 as it is waiting and after that until the stream of a packet data division is completed.
[0174]Thusthe stream of the packet data division by which scramble is carried out is changed into the stream which it comes to descrambleand the stream supplied from the storage medium 81 is transmitted to MPEG decoder 93.
[0175]In MPEG decoder 93the stream of picture image data and the stream of voice data are separated and decrypted from the stream outputted from the descramble circuit 82and it is transmitted to the television receiver 94.
[0176]Thusin the data transmission method of this inventionand the 3rd gestalt of operation of a systemThe standard stream for MPEG 2-PS outputted from MPEG encoder 69It is changed into the stream which carries out the scramble of the stream of the packet data division made into the object of scramble in the scramble circuit 70and via the storage medium 81The descramble circuit 82 is suppliedescrambling is performed and it is transmitted to MPEG decoder 93.
[0177]A stream is changed into a 64-bit parallel stream in the scramble circuit 70 hereFor every stream of the packet data division made into the object of scramble. The same data of PTS of the packet header unit of a packet as the packet data division which is going to carry out scrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which is going to carry out scramble. The scramble of the stream of the packet data division made into the object of scramble is performed by supplying the random number generator 71 among the packet header units in which PTS exists by making the data value of PTS of the last packet header unit into an initial value.

[0178]As a resultin the descramble circuit 82Change a stream into a 64-bit parallel streamand for every stream of the packet data division by which scramble is carried out. The same data of PTS of the packet header unit of a packet as the packet data division which it is going to descrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which it is going to descramble. Descrambling of the stream of the packet data division by which scramble is carried out will be performed by supplying the random number generator 83 among the packet header units in which PTS exists by making the data value of PTS of the last packet header unit into an initial value.
[0179]Thusaccording to the data transmission method of this inventionand the 3rd gestalt of operation of a systemto the random number generator 83 of the descramble circuit 82. The data value of PTS which does not set a data value constant is supplied as an initial value for every stream of the packet data division by which scramble is carried outand. Since the number of times of a random number generation can be made into 1/64it becomes difficult to analyze the random number pattern generated from the random number generator 83and high data transmission of confidentiality can be realized.
[0180]The 4th gestalt .. Drawing 10 drawing 10 is a block diagram showing the important section of the data transmitting system (the 4th gestalt of operation of the data transmitting system of this invention) used for operation of the 4th gestalt of implementation of the data transmission method of this invention.
[0181]97 among drawing 10 A personal computer98 is a PCMCIA (PersonalComputer Memory Card International Association) card based on the PC card standard release 2.0 which constitutes a part of descramble circuit.
[0182]As for CPU (CentralProcessing unit) and 100in the personal computer 97a bus and 102 are PCMCIA interfaces a store circuit and 101 99 here.
[0183]The stream outputted from the scramble circuit 23 which 103 is a disk unit and shows drawing 1 104That isthe disk with which the stream which carries out the scramble of the stream of the packet data division for which the standard stream for MPEG 2-PS is set as the object of scramble was storedand 105 are the disk read features for reading a stream in the disk 104.
[0184]106 inputs the stream read from the disk reader style 105It is a position detecting circuit which performs detection of a packet start codethe check of the contents of PES scramble controlthe check of the contents of the PTS&DTS flagthe detecting position of PTSstarting position detection of a packet data divisionetc.
[0185]The random number generator which generates the random number of a series in which a key signal specifies 107 in PCMCIA card 98108 is a data holding circuit holding PTS dataand this data holding circuit 108 will be controlled by the position detecting circuit 106 to hold the data of this PTS that carried out the detecting positionif the position detecting circuit 106 detects the position of PTS.
[0186]109 is a selection circuitry which supplies the random number itself outputted from the PTS data or the random number generator 107 which the data holding circuit 108 holds to the random number generator 107If the position

detecting circuit 106 detects the object of descramblingi.e.the starting position of a packet data division by which scramble is carried outthis selection circuitry 109It is controlled by the position detecting circuit 106 to feed back the random number outputted from the random number generator 107 until it supplies the random number generator 107 by making into an initial value the PTS data which the data holding circuit 108 holds and the stream of a packet data division is completed after that.

[0187]The inside of the stream to which 110 is supplied from the disk reader style 105It is an EOR circuit which carries out EOR processing of the stream of the packet data division by which scramble is carried outand the random number outputted from the random number generator 107and descrambles the stream of the packet data division by which scramble is carried out.

[0188]111 is a selection circuitry which chooses and outputs the stream supplied from the disk reader style 105and the stream outputted from EOR circuit 110This selection circuitry 111 is controlled by the position detecting circuit 106 to output the stream which changed the stream supplied from the disk reader style 105 into the stream which comes to descramble the stream of the packet data division by which scramble is carried out.

[0189]The store circuit where 112 memorizes ID information (identification data) etc.and 113 are the processing circuits for processing outputting ID information from the store circuit 112 etc.

[0190]Although the descramble circuit comprises the position detecting circuit 106 and PCMCIA card 98 herethis descramble circuit makes the 4th gestalt of operation of the descrambling device of this invention.

[0191]The initial value supply circuit in a descramble circuit comprises the position detecting circuit 106the data holding circuit 108and the selection circuitry 109. Although it may be made to form the position detecting circuit 106 in PCMCIA card 98when providing in the personal computer 97 sideit can reduce the input/output terminal of PCMCIA card 98 like this example.

[0192]In the personal computer 97114 is an MPEG decoder which separates and decrypts the stream of picture image dataand the stream of voice data from the stream outputted from the selection circuitry 111i.e.the stream outputted from PCMCIA card 98.

[0193]The display on which the picture image data in which 115 is outputted from MPEG decoder 114 is suppliedand 116 are loudspeakers to which the voice data outputted from MPEG decoder 114 is supplied.

[0194]When PCMCIA card 98 is inputted into the personal computer 97in this data transmitting system CPU99Make ID information output from PCMCIA card 98judge whether ID information can be attestedand when it can attestThe key signal and the key signal of an identical content which were used in the scramble circuit to the processing circuit 113 are made to generateand it enables it to generate the random number of the series as the random number generator in a scramble circuit with the same random number generator 107.

[0195]And if the disk unit 103 is startedthe stream memorized by the disk 104 will

be outputted from the disk read-out mechanism 105and will be supplied to the position detecting circuit 106the data holding circuit 108 of PCMCIA card 98EOR circuit 110and the selection circuitry 111.
[0196]When the position detecting circuit 106 detects a packet start code hereWhen it judges whether the scramble of the stream of a packet data division is carried out and scramble is not carried out from the contents of scramble control of a packet header unitit returns to the state for detecting a packet start code.
[0197]On the other handwhen the scramble of the stream of a packet data division is carried outthe position detecting circuit 106 judges the existence of whether the PTS&DTS flag of a packet header unit is "10" or "11"and PTS.
[0198]When a PTS&DTS flag is "10" or "11" as a result of judgment (i.e.when PTS exists)the position detecting circuit 106 detects the position of PTSmakes PTS data hold to the data holding circuit 108and will be in the state for detecting the starting position of a packet data division.
[0199]On the other handwhen a PTS&DTS flag is except "10" or "11" (i.e.when PTS does not exist)the position detecting circuit 106 will be in the state for detecting the starting position of a packet data division as it is.
[0200]And if the starting position of a packet data division is detectedthe position detecting circuit 106The PTS data which the data holding circuit 108 holdsi.e.the same data of PTS of the packet header unit of a packet as the packet data division which it is going to descrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which it is going to descramble. The selection circuitry 109 is controlled to supply the random number generator 107 among the packet header units in which PTS exists by making the PTS data of the last packet header unit into an initial value.
[0201]The object of descrambling among the streams supplied here from the disk reader style 105 in EOR circuit 110i.e.the stream of a packet data division by which scramble is carried outEOR processing of the random number outputted from the random number generator 107 is carried outand descrambling of the stream of the packet data division by which scramble is carried out is performed.
[0202]The position detecting circuit 106 controls the selection circuitry 111and it is made to continue outputting the descrambled stream which is outputted from EOR circuit 110It is made to make it output the stream supplied from the disk reader style 105 as it is waiting and after that until the stream of a packet data division is completed.
[0203]Thusthe stream of the packet data division by which scramble is carried out is changed into the stream which it comes to descrambleand the stream supplied from the disk reader style 105 is transmitted to MPEG decoder 114.
[0204]In MPEG decoder 114the stream of picture image data and the stream of voice data are separated and decrypted from the stream supplied from PCMCIA card 98picture image data is transmitted to the display 115and voice data is transmitted to the loudspeaker 116.
[0205]Thusin the data transmission method of this inventionand the 4th gestalt of

operation of a systemThe stream read from the disk 104 with which the stream which carries out the scramble of the stream of the packet data division for which the standard stream for MPEG 2-PS is set as the object of scramble was storedThe descramble circuit which consists of the position detecting circuit 106 and PCMCIA card 98 descrambles.
[0206]In the descramble circuit which consists of the position detecting circuit 106 and PCMCIA card 98 hereThe same data of PTS of the packet header unit of a packet as the packet data division which it is going to descramble for every stream of the packet data division by which scramble is carried outOr when PTS does not exist in the packet header unit of the same packet as the packet data division which it is going to descramble. Descrambling of the stream of the packet data division by which scramble is carried out is performed by supplying the random number generator 107 among the packet header units in which PTS exists by making the data value of PTS of the last packet header unit into an initial value.
[0207]Thusaccording to the data transmission method of this inventionand the 4th gestalt of operation of a systemto the random number generator 107 of PCMCIA card 98. The data value of PTS which does not set a data value constant is supplied as an initial value for every stream of the packet data division by which scramble is carried outand. Since it can be made not to carry out to the random number generator 107 direct access from CPU99it becomes difficult to analyze the random number pattern generated from the random number generator 107and high data transmission of confidentiality can be realized.
[0208]When accounting information can be given to PCMCIA card 98 and it does in this wayfee collection with the information read from the disk 104 is attained.
[0209]The 5th gestalt .. Drawing 11 drawing 11 is a block diagram showing the important section of the data transmitting system (the 5th gestalt of operation of the data transmitting system of this invention) used for operation of the 5th gestalt of implementation of the data transmission method of this invention.
[0210]117 are an MPEG encoder which codes and carries out Time Division Multiplexing of the picture image data obtained with a cameraand the voice data obtained with a microphoneand is encoded to the stream based on an MPEG 2-PS standard or an MPEG 2-TS standard among drawing 11.
[0211]118 is a scramble circuit where the stream of the packet data division made into the object of scramble changes the stream outputted from MPEG encoder 117 into the stream by which scramble was carried out.
[0212]This scramble circuit 118 is a scramble device used for operation of the 4th gestalt of operation of the scrambling method of this inventionand makes the 4th gestalt of operation of the scramble device of this invention.
[0213]In the scramble circuit 118the buffer memory which stores the stream to which 119 is outputted from MPEG encoder 117the memory controller with which 120 controls the buffer memory 119and 121 are buses.
[0214]The random number generator of a DES standard which generates the random number of the series as which 122 is specified by a key signal123 Detection of the packet start code about the standard stream for MPEG 2-PSThe

check of the contents of PES scramble controlthe check of the contents of the PTS&DTS flagThe detecting position of PTSstarting position detection of a packet data divisionand detection of the synchronous byte about the stream of MPEG 2-TSIt is CPU which functions as a position detecting circuit etc. which perform the check of the contents of the adaptation flagthe check of the contents of the pay-load flagthe check of the contents of the PCR flagthe detecting position of PCRstarting position detection of a payload partetc.

[0215]124 is program memory which stores the program for changing the activity of CPU123 by the case where they are a case where the stream outputted from MPEG encoder 117 is an MPEG 2-PS standardand an MPEG 2-TS standard.

[0216]125 is an initial value register which stores the initial value which should be supplied to the random number generator 122When the stream inputted from MPEG encoder 117 is a standard stream for MPEG 2-PSPTS data is storedand in the case of the standard stream for MPEG 2-TSPCR data is stored.

[0217]The selection circuitry which supplies the random number itself outputted from the data value or the random number generator 122 with which the initial value register 125 holds 126 to the random number generator 122and 127 are selection-control registers which control the selection operation of the selection circuitry 126.

[0218]If CPU123 detects here the starting position of the packet data division made into the object of scrambleor a payload partthe selection circuitry 126It is controlled by the output value of the selection-control register 127 to feed back the random number outputted from the random number generator 122 until it supplies the initial value which an initial value register holds to the random number generator 122 and the stream of a packet data division or a payload part is completed after that.

[0219]The data register in which 128 stores the stream read from the buffer memory 119129 carries out EOR processing of the stream of the packet data division outputted from the data register 128or a payload partand the random number outputted from the random number generator 122It is an EOR circuit which carries out the scramble of the stream of the packet data division made into the object of scrambleor a payload part.

[0220]Chooseand 130 is the stream outputted from the data register 128and the stream outputted from EOR circuit 129 a selection circuitry to outputand this selection circuitry 130It is controlled to output the stream from which the stream of the packet data division made into the object of scramble or the payload part changed the stream outputted from the data register 128 into the stream which comes to carry out scramble.

[0221]131 is storage mediasuch as a disk which accumulates the stream outputted from the selection circuitry 130i.e.the stream outputted from the scramble circuit 118.

[0222]132 is a descramble circuit where the stream of the packet data division by which scramble is carried outor a payload part changes the stream supplied from the storage medium 131 into the stream which it comes to descramble.

[0223]This descramble circuit 132 is a descrambling device used for operation of the 5th gestalt of implementation of the descrambling method of this inventionand makes the 5th gestalt of operation of the descrambling device of this invention.
[0224]In this descramble circuit 132the buffer memory which stores the stream to which 133 is outputted from the storage medium 131the memory controller with which 134 controls the buffer memory 133and 135 are buses.
[0225]136 is a random number generator of the same circuitry as the random number generator 122and the key signal and the key signal of an identical content which were used for the random number generator 122 are supplied to this random number generator 136.
[0226]137 Detection of the packet start code about the standard stream for MPEG 2-PSThe check of the contents of PES scramble controlthe check of the contents of the PTS&DTS flagThe detecting position of PTSstarting position detection of a packet data divisionand detection of the synchronous byte about the standard stream for MPEG 2-TSIt is CPU which functions as a position detecting circuit etc. which perform the check of the contents of the adaptation flagthe check of the contents of the pay-load flagthe check of the contents of the PCR flagthe detecting position of PCRstarting position detection of a payload partetc.
[0227]138 is program memory which stores the program for changing the activity of CPU137 by the case where they are a case where the stream supplied from the storage medium 131 is an MPEG 2-PS standardand an MPEG 2-TS standard.
[0228]139 is an initial value register which stores the initial value which should be supplied to the random number generator 136When the stream supplied from the storage medium 131 is a standard stream for MPEG 2-PSPTS data is storedand in the case of the standard stream for MPEG 2-TSPCR data is stored.
[0229]The selection circuitry which supplies the random number itself outputted from the data value or the random number generator 136 with which the initial value register 139 holds 140 to the random number generator 136and 141 are selection-control registers which control the selection operation of the selection circuitry 140.
[0230]If CPU137 detects here the starting position of the packet data division by which scramble is carried outor a payload partthe selection circuitry 140It is controlled by the output value of the selection-control register 141 to feed back the random number outputted from the random number generator 136 until it supplies the initial value which the initial value register 139 holds to the random number generator 136 and the stream of a packet data division or a payload part is completed after that.
[0231]The data register in which 142 stores the stream read from the buffer memory 133143 carries out EOR processing of the stream of the packet data division outputted from the data register 142or a payload partand the random number outputted from the random number generator 136It is an EOR circuit which descrambles the stream of the packet data division by which scramble is carried outor a payload part.

[0232]Chooseand 144 is the stream outputted from the data register 142and the stream outputted from EOR circuit 143 a selection circuitry to outputand this selection circuitry 144It is controlled to output the stream which changed the stream outputted from the data register 142 into the stream which comes to descramble the stream of the packet data division by which scramble is carried outor a payload part.
[0233]145 is an MPEG decoder which separates and decrypts the stream of picture image dataand the stream of voice data from the stream outputted from the descramble circuit 132.
[0234]In this data transmitting systemthe picture image data obtained with a cameraand the voice data obtained with a microphoneBy MPEG encoder 117it is encoded by the stream based on an MPEG 2-PS standard or an MPEG 2-TS standardand is transmitted to the scramble circuit 118.
[0235]And the stream which the stream supplied to the scramble circuit 118 was stored in the buffer memory 119and was stored in the buffer memory 119 is read by CPU123.
[0236]When the stream outputted here from MPEG encoder 117 is a standard stream for MPEG 2-PSCPU123 performs detection of a packet start codethe check of the contents of PES scramble controlthe check of the contents of PTS&DTSthe detecting position of PTSstarting position detection of a packet data divisionetc.
[0237]And when CPU123 detects a packet start codethe stream of a packet data division judges whether it is considered as the object of scramble from the contents of scramble control of a packet header unitWhen not considered as the object of scrambleit returns to the state for detecting a packet start code.
[0238]On the other handwhen the stream of the packet data division is made into the object of scrambleCPU123 judges the existence of whether the PTS&DTS flag of a packet header unit is "10" or "11"and PTS.
[0239]When a PTS&DTS flag is "10" or "11" as a result of judgment (i.e.when PTS exists)CPU123 detects the position of PTSmakes PTS data hold to the initial value register 125and will be in the state for detecting the starting position of a packet data division.
[0240]On the other handwhen a PTS&DTS flag is except "10" or "11" (i.e.when PTS does not exist)CPU123 will be in the state for detecting the starting position of a packet data division as it is.
[0241]And if the starting position of a packet data division is detectedCPU123The PTS data which the initial value register 125 holdsi.e.the same data of PTS of the packet header unit of a packet as the packet data division which is going to carry out scrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which is going to carry out scramble. The selection-control register 127 is rewritten so that the random number generator 122 may be supplied among the packet header units in which PTS exists by making the PTS data of the last packet header unit into an initial value.
[0242]The stream of the packet data division made into the object of scramble

among the streams outputted here from the data register 128 in EOR circuit 129EOR processing of the random number outputted from the random number generator 122 is carried outand the scramble of the stream of the packet data division made into the object of scramble is performed.
[0243]In this caseCPU123 controls the selection circuitry 130makes it continue outputting the stream which is outputted from EOR circuit 129 and by which scramble was carried outand it returns to the state for detecting waiting and a packet start code until the stream of a packet data division is completed.
[0244]Thusthe stream outputted from MPEG encoder 117The stream which the stream of the packet data division made into the object of scramble was changed into the stream which comes to carry out scramblewas accumulated in the storage medium 131and was accumulated in this storage medium 131 will be suitably supplied to the descramble circuit 132.
[0245]The stream which the stream supplied to the descramble circuit 132 was stored in the buffer memory 133and was stored in the buffer memory 133 is read here by CPU137.
[0246]And CPU137 judges whether the scramble of the stream of a packet data division is carried out from the contents of scramble control of a packet header unitwhen a packet start code is detectedWhen scramble is not carried outit returns to the state for detecting a packet start code.
[0247]On the other handwhen the scramble of the stream of a packet data division is carried outCPU137 judges the existence of whether the PTS&DTS flag of a packet header unit is "10" or "11"and PTS.
[0248]When a PTS&DTS flag is "10" or "11" as a result of judgment (i.e.when PTS exists)CPU137 detects the position of PTSmakes PTS data hold to the initial value register 139and will be in the state for detecting the starting position of a packet data division.
[0249]On the other handwhen a PTS&DTS flag is except "10" or "11" (i.e.when PTS does not exist)CPU137 will be in the state for detecting the starting position of a packet data division as it is.
[0250]And if the starting position of a packet data division is detectedCPU137The PTS data which the initial value register 139 holdsi.e.the same data of PTS of the packet header unit of a packet as the packet data division which it is going to descrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which it is going to descramble. The selection-control register 141 is rewritten so that the random number generator 136 may be supplied among the packet header units in which PTS exists by making the PTS data of the last packet header unit into an initial value.
[0251]The stream of the packet data division by which scramble is carried out among the streams outputted here from the data register 142 in EOR circuit 143EOR processing of the random number outputted from the random number generator 136 is carried outand descrambling of the stream of the packet data division by which scramble is carried out is performed.
[0252]In this caseCPU137 controls the selection circuitry 144makes it continue

outputting the descrambled stream which is outputted from EOR circuit 143and it returns to the state for detecting waiting and a packet start code until the stream of a packet data division is completed.
[0253]Thusthe stream of the packet data division made into the object of scramble is changed into the stream which comes to carry out scrambleand the stream outputted from the storage medium 131 is transmitted to MPEG decoder 145.
[0254]On the other handwhen the standard stream for MPEG 2-TS is outputted from MPEG encoder 117. CPU123 returns to the state for detecting a synchronous bytewhen a synchronous byte is detectedthe stream of a payload part judges whether it is considered as the object of scramble from the contents of scramble control of a packet header unit and it is not made into the object of scramble.
[0255]On the other handwhen the stream of the payload part is made into the object of scramble. When it judges whether CPU123 has the adaptation field from an adaptation flag and there is no adaptation fieldCPU123 judges whether there is any pay load from a pay-load flag.
[0256]On the other handwhen CPU123 judges whether there is PCR from an PCR flag when there is the adaptation fieldand there is no PCRit is judged whether there is any pay load from a pay-load flag.
[0257]On the other handwhen there is PCRCPU123 detects the position of PCRmakes PCR data hold to the initial value register 125and judges whether there is any pay load from a pay-load flag.
[0258]When CPU123 will be in the state for detecting a synchronous byte when there is no pay load and a pay load is hereit will be in the state for detecting the starting position of a payload part.
[0259]And the PCR data which the initial value register 125 will hold if CPU123 detects the starting position of a payload partNamelythe data of the same PCR of the packet header unit of a packet as the payload part which is going to carry out scrambleOr when PCR does not exist in the packet header unit of the same packet as the payload part which is going to carry out scramble. The selection-control register 127 is rewritten so that the random number generator 122 may be supplied among the packet header units in which PCR exists by making the PCR data of the last packet header unit into an initial value.
[0260]The stream of the payload part made into the object of scramble among the streams outputted here from the data register 128 in EOR circuit 129EOR processing of the random number outputted from the random number generator 122 is carried outand the scramble of the stream of the payload part made into the object of scramble is performed.
[0261]In this caseCPU123 controls the selection circuitry 130makes it continue outputting the stream which is outputted from EOR circuit 129 and by which scramble was carried outand it returns to the state for detecting waiting and a synchronous byte until the stream of a payload part is completed.
[0262]Thusthe stream outputted from MPEG encoder 117The stream which the

stream of the packet data division made into the object of scramble was changed into the stream which comes to carry out scramblewas accumulated in the storage medium 131and was accumulated in this storage medium 131 will be suitably supplied to the descramble circuit 132.
[0263]The stream which the stream supplied to the descramble circuit 132 was stored in the buffer memory 133and was stored in the buffer memory 133 is read here by CPU137.
[0264]Herea synchronous byte is detectedCPU137 judges whether the scramble of the stream of a payload part is carried out from the contents of scramble control of a packet header unitand when scramble is not carried out hereit returns to the state for detecting a synchronous byte.
[0265]On the other handwhen the scramble of the stream of a payload part is carried out. CPU137 judges whether there is any pay load from a pay-load flagwhen it judges whether there is any adaptation field from an adaptation flag and there is no adaptation field.
[0266]On the other handwhen CPU137 judges whether there is PCR from an PCR flag when there is the adaptation fieldand there is no PCRit is judged whether there is any pay load from a pay-load flag.
[0267]On the other handwhen there is PCRCPU137 detects the position of PCRmakes PCR data hold to the initial value register 139and judges whether there is any pay load from a pay-load flag.
[0268]When CPU137 will be in the state for detecting a synchronous byte when there is no pay load and a pay load is hereit will be in the state for detecting the starting position of a payload part.
[0269]And the PCR data which the initial value register 139 will hold if CPU137 detects the starting position of a payload partNamelythe data of the same PCR of the packet header unit of a packet as the payload part which it is going to descrambleOr when PCR does not exist in the packet header unit of the same packet as the payload part which it is going to descramble. The selection-control register 141 is rewritten so that the random number generator 136 may be supplied among the packet header units in which PCR exists by making the PCR data of the last packet header unit into an initial value.
[0270]The stream of the payload part by which scramble is carried out among the streams outputted here from the data register 142 in EOR circuit 143EOR processing of the random number outputted from the random number generator 136 is carried outand descrambling of the stream of the payload part by which scramble is carried out is performed.
[0271]In this caseCPU137 controls the selection circuitry 144makes it continue outputting the descrambled stream which is outputted from EOR circuit 143and it returns to the state for detecting waiting and a synchronous byte until the stream of a payload part is completed.
[0272]Thusin the descramble circuit 132the stream of the payload part by which scramble is carried out is changed into the stream which it comes to descrambleand the stream outputted from the storage medium 131 is transmitted

to MPEG decoder 145.
[0273]Thusin the data transmission method of this inventionand the 5th gestalt of operation of a systemThe stream the MPEG 2-PS standard outputted from MPEG encoder 117 or standard for MPEG 2-TSIn the scramble circuit 118it is changed into the stream which carries out the scramble of the stream of a packet data division or a payload partand via the storage medium 131the descramble circuit 132 is suppliedescrambling is performedand it is transmitted to MPEG decoder 145.
[0274]In the scramble circuit 118 hereFor every stream of the packet data division made into the object of scrambleor a payload part. The same data of PTS of the packet header unit of a packet as the packet data division which is going to carry out scrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which is going to carry out scramble. The PTS data of the packet header unit of the just before of the packet header units in which PTS existsOr the data of the same PCR of the packet header unit of a packet as the payload part which is going to carry out scrambleOr when PCR does not exist in the packet header unit of the same packet as the payload part which is going to carry out scramble. The scramble of the stream of the packet data division made into the object of scramble or a payload part is performed by supplying the random number generator 122 among the packet header units in which PCR exists by making the PCR data of the last packet header unit into an initial value.
[0275]As a resultin the descramble circuit 132For every stream of the packet data division by which scramble is carried outor a payload part. The same data of PTS of the packet header unit of a packet as the packet data division which it is going to descrambleOr when PTS does not exist in the packet header unit of the same packet as the packet data division which it is going to descramble. The PTS data of the packet header unit of the just before of the packet header units in which PTS existsOr the data of the same PCR of the packet header unit of a packet as the payload part which it is going to descrambleOr when PCR does not exist in the packet header unit of the same packet as the payload part which it is going to descramble. Descrambling of the stream of the packet data division made into the object of descrambling or a payload part is performed by supplying the random number generator 122 among the packet header units in which PCR exists by making the PCR data of the last packet header unit into an initial value.
[0276]Thusaccording to the data transmission method of this inventionand the 5th gestalt of operation of a systemto the random number generator 136 of the descramble circuit 132. Since the data value of PTS which does not set a data value constantor PCR will be supplied as an initial value for every stream of the packet data division by which scramble is carried outor a payload partSince it becomes difficult to analyze the random number pattern generated from the random number generator 136and high data transmission of confidentiality can be realized and it is applicable to the transmission system of two series of an MPEG 2-PS system and an MPEG 2-TS systemconvenience can be improved.

[0277]
[Effect of the Invention]As mentioned abovein using the scrambling method of this invention. Descrambling every 2nd stream part by which scramble is carried out. When the 1st data value of stream circles supplies a random number generator by making into an initial value the predetermined data which is not constantit will be carried out and to the random number generator by the side of descrambling. Since the initial value which does not set a value constant will be supplied every 2nd stream part by which scramble is carried outit becomes difficult to analyze the random number pattern generated from a random number generatorand high data transmission of confidentiality can be realized.
[0278]In using the scramble device of this inventionA descrambling device every 2nd stream part by which scramble is carried out to the random number generator which generates a random number. The initial value supply circuit supplied to a random number generator by making into an initial value the predetermined data whose 1st data value of stream circles is not constantWill have a logic operation circuit which descrambles the 2nd stream part by which scramble is carried out by carrying out the logical operation of the 2nd stream part by which scramble is carried outand the random number outputted from a random number generatorand it will be constitutedSince the initial value which does not set a value constant will be supplied every 2nd stream part by which scramble is carried out to the random number generator of the descrambling deviceit becomes difficult to analyze the random number pattern generated from a random number generatorand high data transmission of confidentiality can be realized.
[0279]According to the descrambling method of this inventionto a random number generator. Since the initial value which does not set a value constant will be supplied every 2nd stream part by which scramble is carried outit becomes difficult to analyze the random number pattern generated from a random number generatorand high data transmission of confidentiality can be realized.
[0280]According to the descrambling device of this inventionto a random number generator. Since the initial value which does not necessarily set a value constant will be supplied every 2nd stream part by which scramble is carried outit becomes difficult to analyze the random number pattern generated from a random number generatorand high data transmission of confidentiality can be realized.
[0281]Since the scrambling method of this invention and the descrambling method of this invention are used according to the data transmission method of this inventionthe high data transmission of confidentiality is realizable.
[0282]Since the scramble device of this invention and the descrambling device of this invention are used according to the data transmission device of this inventionthe high data transmission of confidentiality is realizable.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a block diagram showing the important section of the data transmitting system (the 1st gestalt of operation of the data transmitting system of this invention) used for operation of the 1st gestalt of implementation of the data transmission method of this invention.
[Drawing 2]It is a figure showing the structure of the PES packet of MPEG 2-PS.
[Drawing 3]It is a flow chart for explaining operation of the scramble circuit with which the 1st gestalt of operation of the data transmitting system of this invention shown in drawing 1 is provided.
[Drawing 4]It is a flow chart for explaining operation of the descramble circuit with which the 1st gestalt of operation of the data transmitting system of this invention shown in drawing 1 is provided.
[Drawing 5]It is a block diagram showing the important section of the data transmitting system (the 2nd gestalt of operation of the data transmitting system of this invention) used for operation of the 2nd gestalt of implementation of the data transmission method of this invention.
[Drawing 6]It is a figure showing the structure of the transport packet of MPEG 2-TS.
[Drawing 7]It is a flow chart for explaining operation of the scramble circuit with which the 2nd gestalt of operation of the data transmitting system of this invention shown in drawing 5 is provided.
[Drawing 8]It is a flow chart for explaining operation of the descramble circuit with which the 2nd gestalt of operation of the data transmitting system of this invention shown in drawing 5 is provided.
[Drawing 9]It is a block diagram showing the important section of the data transmitting system (the 3rd gestalt of operation of the data transmitting system of this invention) used for operation of the 3rd gestalt of implementation of the data transmission method of this invention.
[Drawing 10]It is a block diagram showing the important section of the data transmitting system (the 4th gestalt of operation of the data transmitting system of this invention) used for operation of the 4th gestalt of implementation of the data transmission method of this invention.
[Drawing 11]It is a block diagram showing the important section of the data transmitting system (the 5th gestalt of operation of the data transmitting system of this invention) used for operation of the 5th gestalt of implementation of the data transmission method of this invention.
[Drawing 12]It is a block diagram showing the important section of an example of the conventional data transmitting system.
[Drawing 13]It is a figure for explaining the problem which the data transmitting system shown in drawing 12 has.
[Description of Notations]
224369117 MPEG encoders
386493114145 MPEG decoders
234470118 scramble circuits

315782132 descramble circuits